What is claimed is:

1. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through monitors disposed at a plurality of points in the network; and

communicating data from the monitors, over a hardened, redundant network, to a central controller.

2. The method of claim 1 wherein the hardened redundant network is inaccessible to the attacker.

3. The method of claim 1 further comprising:

monitoring network traffic through a gateway that passes network packets, the gateway being disposed at an edge of the network to protect the data center, with the gateway coupled to the control center by the redundant hardened network.

4. The method of claim 1 further comprising:

analyzing network traffic statistics to identify malicious network traffic; and

filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious network traffic during analyzing of the network traffic.

5. The method of claim 1 wherein the gateway is located at network entry points of victim data centers.

6. The method of claim 1 further comprising:

performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

7. The method of claim 3 wherein performing intelligent traffic analysis and filtering is performed by the gateways and the control center.

8. The method of claim 3 wherein the gateways perform intelligent traffic analysis and filtering.

9. The method of claim 1 wherein the monitors include data collectors that sample packet traffic, accumulate, and collect statistical information about network flows.

10. The method of claim 9 wherein the data collectors are located at major peering points and network points of presence.

11. The method of claim 1 wherein the control center aggregates traffic information and coordinates measures to track down and block the sources of an attack.

12. A distributed system to thwarting denial of service attacks comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data for performance of intelligent traffic analysis and filtering to identify malicious traffic and to eliminate the malicious traffic to thwart the denial of service attack.

13. The distributed system of claim 12 further comprising:

a control center coupled to the plurality of data collectors by a hardened redundant connection to communicate the data to the control center; and wherein the control centers performs the intelligent traffic analysis to identify the malicious traffic.

14. The distributed system of claim 13 further comprising:

at least one gateway device that passes network packets between the network and the victim site, the gateway disposed to protect a victim site, and being coupled to the control center by the redundant hardened network.

15. A system for thwarting denial of service attacks on a victim data center coupled to a network comprises:

a first plurality of monitors that monitor network traffic flow through the network, the first plurality of monitors disposed at a second plurality of points in the network; and

a central controller that receives data from the plurality of monitors, over a hardened, redundant network, the central controller analyzing network traffic statistics to identify malicious network traffic.

16. The system of claim 15 wherein the hardened redundant network is inaccessible to the attacker.

17. The system of claim 15 further comprising:

at least one gateway that passes network packets between the network and the victim data center, the gateway disposed to protect potential victim data center and being

coupled to the control center by the redundant hardened network.

18. The system of claim 17 wherein the gateway is disposed at an edge of the network at victim data center.

19. The system of claim 17 wherein the gateway analyzes network traffic statistics to identify malicious network traffic and filters the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious network traffic during analyzing of the network traffic.

20. The system of claim 17 wherein the gateway is located at the edge of the network that is an entry point to the victim data center.

21. The system of claim 17 wherein both the gateway and the control center perform intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

22. The system of claim 15 wherein the data collectors sample packet traffic, and accumulate and collect statistical information about network flows.

23. The system of claim 15 wherein the data collectors are located at major peering points and network points of presence.

24. The system of claim 17 wherein the data collectors sample packet traffic, and accumulate and collect

statistical information about network flows and are located at major peering points and network points of presence.

25. The system of claim 17 wherein the control center aggregates traffic information and coordinates measures to track down and block the sources of an attack.

26. The system of claim 17 wherein the gateway includes a process to communicate with the control center over the hardened network.

27. The system of claim 17 wherein the gateway includes a process to allow an administrator to insert filters to discard packets that are deemed to be part of an attack, as determined by heuristics of the traffic flow.

28. A distributed system to thwart denial of service attacks comprises:

a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering identify malicious traffic at the source of an attack to eliminate the malicious traffic and thwart the denial of service attack.